SYSTEM, APPARATUS AND METHOD FOR REPLACING A CRYPTOGRAPHIC KEY

ABSTRACT

Embodiments describe a method and/or system whereby a secret key in a cryptographic system may be replaced without revealing the secret key. One embodiment comprises creating a first private key and corresponding first public key. A second private key associated with the first private key and a second public key corresponding to the second private key are also created. The second private key is output once such that it can be re-created and the second public key is output when outputting the first public key. The first private key is used for authentication. The method further comprises re-creating the second private key; and using the second private key for authentication. Another embodiment comprises creating a private key and corresponding public key with associated system parameter; outputting the system parameter when outputting the public key; and using the private key for authentication. The method may further comprise creating a new private key using the previous key and the system parameter.